Attorney's Docket No. 5683P013 Patent

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:

Andrew Augustine WAJS, et al.

Application No.: New application

Filed: Herewith

For: METHOD FOR OPERATING A CONDITIONAL ACCESS SYSTEM FOR BROADCAST APPLICATIONS

National Phase Filing of:

PCT/EP 00/13394

filed 18 December 2000

Examiner: Not yet assigned

Art Group: Not yet assigned

Assistant Commissioner of Patents
Washington, DC 20231-9998

PRELIMINARY AMENDMENT

Sir:

Applicant respectfully requests the Examiner to enter the following amendments.

IN THE CLAIMS:

Please amend the claims as follows:

1. A method for operating a conditional access system for broadcast applications, said conditional access system comprising a number of subscribers, each subscriber having a terminal including a conditional access module and a secure device to store entitlements, wherein a source signal is encrypted using a first key (C_W), said first key (C_W) being changed at a high rate, said encrypted source signal being broadcasted for

receipt by the terminals, wherein entitlement control messages (ECM's) are sent to the secure devices, said ECM's comprising the first keys (C_W) encrypted using a service key (P_T), wherein entitlement management messages (EMM's) are sent to the secure device providing the service key (P_T) required to decrypt encrypted first keys (C_W), wherein a cracked secure device which is used in an unauthorized manner is traced by sending different keys required to obtain the first keys to different terminals or groups of terminals and monitoring the key information provided by a pirate, wherein search EMM's are sent to at least a part of the terminals, said search EMM's providing at least the service key (P_T) and a dummy key (P_{D1} or P_{D2}), at least the search EMM's comprising identifiers identifying the keys (P_T and P_{D1} or P_{D2}), wherein first search EMM's with the keys (P_T and P_{D1}) are sent to a first part of the terminals and second search EMM's with the keys (P_T and P_{D2}) are sent to a second part of the terminals, wherein an ECM identifying the service key (P_T) to be used to decrypt the encrypted first key (C_W), is sent to all secure devices just before the first key (C_W) is needed to decrypt the source signal.

2. A method according to claim 1, wherein the encrypted source signal comprises a stream of data packets, wherein successive groups including at least one data packet, are encrypted using successive first key (C_{W1}, C_{W2},..., C_{Wi},...,C_{Wn}), each data packet having a flag indicating the first key (C_{Wi}) to be used for decrypting the data packet, wherein in stead of an ECM identifying the service key (P_T) an ECM identifying a dummy key (P_{D1} or P_{D2}) to be used identifying a dummy key (C_{Wi}), is sent to the secure devices of the first and second parts of the terminals, respectively, just before the first key (C_{Wi}) is needed to decrypt the source signal, whereas the data packet is encrypted using the previous first key (C_{Wi-1}).

3. A method according to claim 1, wherein a set of search EMM's is sent to the terminals, each search EMM providing two keys (P_T and P_{D1}, PT and P_{D2},..., P_T and P_{Dn}).

4. A method for operating a conditional access system for broadcast applications, said conditional access system comprising a number of subscribers, each subscriber having a terminal including a conditional access module and a secure device to store entitlements, wherein a source signal is encrypted using a first key (C_W), said first key (C_W) being changed at a high rate, said encrypted source signal being broadcasted for receipt by the terminals, wherein entitlement control messages (ECM's) are sent to the secure devices, said ECM's comprising the first keys (C_W) encrypted using a service key (P_T), wherein entitlement management messages (EMM's) are sent to the secure device providing the service key (P_T) required to decrypt encrypted first keys (C_W), wherein a cracked secure device which is used in an unauthorized manner is traced by sending different keys required to obtain the first keys to different terminals or groups of terminals and monitoring the key information provided by a pirate, wherein a set of search EMM's is sent to at least a part of the terminals, each search EMM of the set comprising a different dummy key (P_D) and each EMM being sent to a different part of the terminals.

5. A method according to claim 3, wherein the terminals are divided into groups, wherein in a first search step the number of search EMM's of the set of search EMM's corresponds to the number of groups.

6. A method for operating a conditional access system for broadcast applications, said conditional access system comprising a number of subscribers, each subscriber having a terminal including a conditional access module and a secure device to store

entitlements, wherein a source signal is encrypted using a first key (C_W), said first key (C_W) being changed at a high rate, said encrypted source signal being broadcasted for receipt by the terminals, wherein entitlement control messages (ECM's) are sent to the secure devices, said ECM's comprising the first keys (C_W) encrypted using a service key (P_T), wherein entitlement management messages (EMM's) are sent to the secure device providing the service key (P_T) required to decrypt encrypted first keys (C_W), wherein a cracked secure device which is used in an unauthorized manner is traced by sending different keys required to obtain the first keys to different terminals or groups of terminals and monitoring the key information provided by a pirate, wherein the source signal or the ECM's are encrypted using a multiple-key or secret-sharing cryptographic algorithm having a plurality of different decrypting keys or shares (C_i;P_i) required for decrypting the encrypted source signal or ECM's respectively, wherein said plurality of different decrypting keys or shares (C_i;P_i) are sent to at least a part of the terminals such that different terminals or groups of terminals receive different keys or shares (C_i;P_i) according to a predetermined distribution.

7. A method according to claim 1, wherein the distribution of the terminals in groups of terminals is varied to trace the cracked secure device.

REMARKS

If there are any additional charges, please charge Deposit Account No. 02-2666. If a telephone interview would in any way expedite the prosecution of the present application, the Examiner is invited to contact André L. Marais at (408) 947-8200.

Respectfully submitted,

BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP

Dated: 08/21/, 2001

André L. Marais
Reg. No. 48,095

12400 Wilshire Blvd.
Seventh Floor
Los Angeles, CA 90025-1026
(408) 947-8200

VERSION OF SPECIFICATION AND CLAIMS WITH MARKINGS:

IN THE CLAIMS:

Please amend the claims as follows:

4. (Amended) [Method] A method for operating a conditional access system for broadcast applications, said conditional access system comprising a number of subscribers, each subscriber having a terminal including a conditional access module and a secure device [for storing] to store entitlements, wherein a source signal is encrypted using a first key (C_W), said first key (C_W) being changed at a high rate, said encrypted source signal being broadcasted for receipt by the terminals, wherein entitlement control messages (ECM's) are sent to the secure devices, said ECM's comprising the first keys (C_W) encrypted using a service key (P_T), wherein entitlement management messages (EMM's) are sent to the secure device providing the service key (P_T) required to decrypt encrypted first keys (C_W), wherein a cracked secure device which is used in an unauthorized manner is traced by sending different keys required to obtain the first keys to different terminals or groups of terminals and monitoring the key information provided by a pirate, [characterized in that] wherein search EMM's are sent to at least a part of the terminals, said search EMM's providing at least the service key (P_T) and a dummy key (P_{D1} or P_{D2}), at least the search EMM's comprising identifiers identifying the keys (P_T and P_{D1} or P_{D2}), wherein first search EMM's with the keys (P_T and P_{D1}) are sent to a first part of the terminals and second search EMM's with the keys (P_T and P_{D2}) are sent to a second part of the terminals, wherein an ECM identifying the service key (P_T) to be used to decrypt the encrypted first key (C_W), is sent to all secure devices just before the first key (C_W) is needed to decrypt the source signal.

5. (Amended) [Method] A method according to claim 1, wherein the encrypted source signal comprises a stream of data packets, wherein successive groups including

at least one data packet, are encrypted using successive first key (C_{W1}, C_{W2},..., C_{Wi},...,C_{Wn}), each data packet having a flag indicating the first key (C_{Wi}) to be used for decrypting the data packet, wherein in stead of an ECM identifying the service key (P_T) an ECM identifying a dummy key (P_{D1} or P_{D2}) to be used identifying a dummy key (C_{Wi}), is sent to the secure devices of the first and second parts of the terminals, respectively, just before the first key (C_{Wi}) is needed to decrypt the source signal, whereas the data packet is encrypted using the previous first key (C_{Wi-1}).

6. (Amended) [Method] A method according to claim 1 [or 2], wherein a set of search EMM's is sent to the terminals, each search EMM providing two keys (P_T and P_{D1}, PT and P_{D2},..., P_T and P_{Dn}).

4. (Amended) [Method according to the preamble of claim 1,] A method for operating a conditional access system for broadcast applications, said conditional access system comprising a number of subscribers, each subscriber having a terminal including a conditional access module and a secure device to store entitlements, wherein a source signal is encrypted using a first key (C_W), said first key (C_W) being changed at a high rate, said encrypted source signal being broadcasted for receipt by the terminals, wherein entitlement control messages (ECM's) are sent to the secure devices, said ECM's comprising the first keys (C_W) encrypted using a service key (P_T), wherein entitlement management messages (EMM's) are sent to the secure device providing the service key (P_T) required to decrypt encrypted first keys (C_W), wherein a cracked secure device which is used in an unauthorized manner is traced by sending different keys required to obtain the first keys to different terminals or groups of terminals and monitoring the key information provided by a pirate, wherein a set of search EMM's is sent to at least a part of the terminals, each search EMM of the set

comprising a different dummy key (P_D) and each EMM being sent to a different part of the terminals.

5. (Amended) [Method] A method according to claim 3 [or 4], wherein the terminals are divided into groups, wherein in a first search step the number of search EMM's of the set of search EMM's corresponds to the number of groups.

6. (Amended) [Method according to the preamble of claim 1,] A method for operating a conditional access system for broadcast applications, said conditional access system comprising a number of subscribers, each subscriber having a terminal including a conditional access module and a secure device to store entitlements, wherein a source signal is encrypted using a first key (C_W), said first key (C_W) being changed at a high rate, said encrypted source signal being broadcasted for receipt by the terminals, wherein entitlement control messages (ECM's) are sent to the secure devices, said ECM's comprising the first keys (C_W) encrypted using a service key (P_T), wherein entitlement management messages (EMM's) are sent to the secure device providing the service key (P_T) required to decrypt encrypted first keys (C_W), wherein a cracked secure device which is used in an unauthorized manner is traced by sending different keys required to obtain the first keys to different terminals or groups of terminals and monitoring the key information provided by a pirate, wherein the source signal or the ECM's are encrypted using a multiple-key or secret-sharing cryptographic algorithm having a plurality of different decrypting keys or shares ($C_i;P_i$) required for decrypting the encrypted source signal or ECM's respectively, wherein said plurality of different decrypting keys or shares ($C_i;P_i$) are sent to at least a part of the terminals such that different terminals or groups of terminals receive different keys or shares ($C_i;P_i$) according to a predetermined distribution.

7. (Amended) [Method] A method according to [any one of the preceding claims] claim 1, wherein the distribution of the terminals in groups of terminals is varied to trace the cracked secure device.